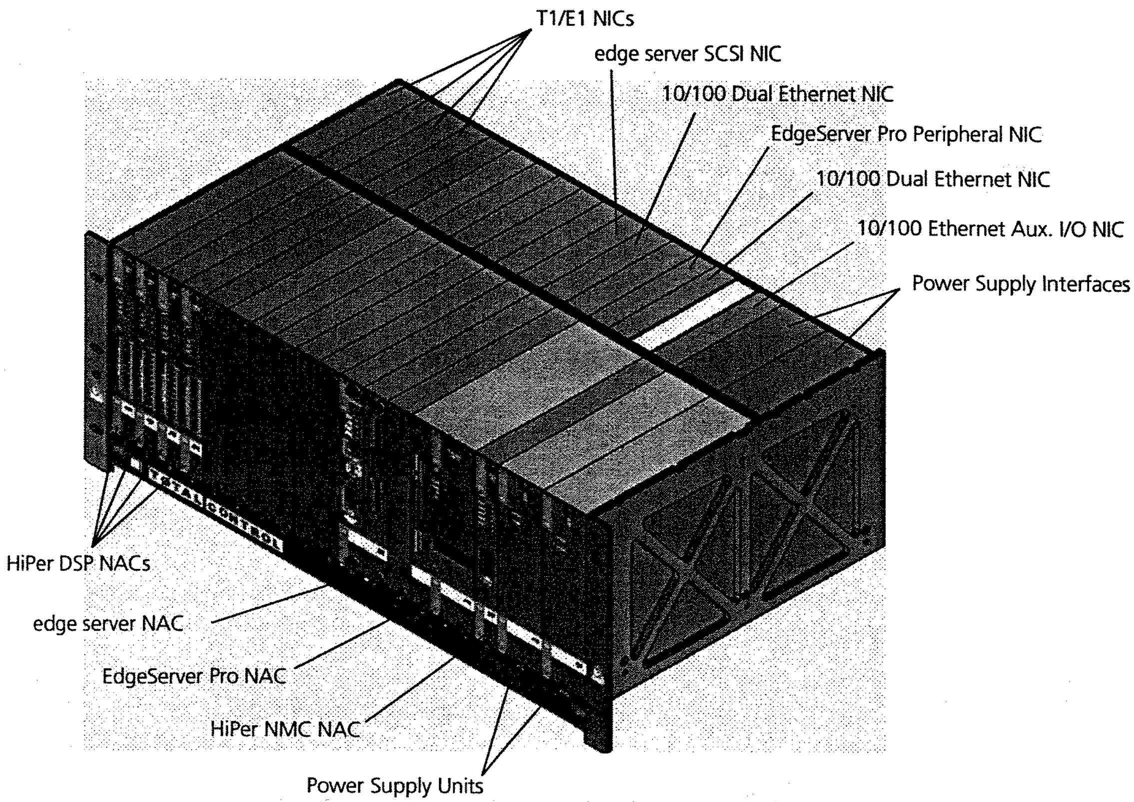
Figure 4 Basic Media Gateway Chassis Configuration



This basic Media Gateway configuration has the following cards installed in the chassis, as shown in Figure 4:

- EdgeServer Pro NAC with a 10/100 Dual Ethernet NIC and an EdgeServer Pro Peripheral NIC
- Edge server NAC with a 10/100 Dual Ethernet NIC and an edge server SCSI NIC
- HiPer Network Management Card (HiPer NMC) NAC with a 10/100 Ethernet Auxiliary I/O NIC
- HiPer DSP NACs with HiPer DSP T1/E1 NICs
- Two 130 Amp Power Supply Units (PSUs) with Power Supply Interfaces.

For the purposes of illustration, both the edge server and the EdgeServer Pro cards are shown in this figure. Only one Gateway card set is required for the configuration shown here.

Call Models The CommWorks IP Telephony media Gateway supports transparent trunking call models.

Transparent Trunking

Transparent trunking, or one-stage calls, are calls that have a dialed number and a prefix string. When the beginning of the dialed number string matches the prefix string, the matched portion is stripped off and the remaining string is used for Dialed Number Identification Service (DNIS)-routing.

Default CODEC for Voice Calls

The Media Gateway supports configuration of a default Media Gateway CODEC that is used for all voice calls. This parameter is set using IP Telephony Manager to configure the CommWorks Media Gateway entity. The default CODEC parameter is sent to the HiPer DSP card at the start of every call. The HiPer DSP card initializes a default CODEC type whenever a reset occurs.

The Default CODEC setting controls the call type support as defined in Table 4 below.

Table 4 CODEC Call Type Support

CODEC	Voice	FAX	Data
G.711	Yes	Yes	Yes
G.723.1	Yes	via T.38	No
G.729A	Yes	via T.38	No

Real-time Gateway Operating Statistics

The edge server card in the Media Gateway runs a Web server that provides operating statistics and event log messages in real time. You can use the Web server without disrupting call processing.

Access the Web server by using the IP address of the edge server card and any web browser that is on the same IP network as the edge server card.

Edge Server Card Sets

Unless otherwise specified, this document uses the generic term edge server to refer to either the EdgeServer Pro or the edge server.

The EdgeServer Pro card set runs the Microsoft Windows NT 4.0 Server operating system and uses two NICs for network, peripheral, and input devices. The Peripheral NIC has keyboard, video, and mouse ports for initial configuration. It also has an Ultra-wide SCSI port for additional peripheral devices such as an external CD-ROM or hard-disk drive.

The edge server card set runs the Microsoft Windows 2000 Server operating system and uses one or two NICs for network and peripheral devices. The Peripheral NIC has an Ultra-wide SCSI port for additional peripheral devices such as an external CD-ROM or hard-disk drive. Keyboard, mouse, video, and USB ports are on the front of the edge server NAC.

Both edge servers use a Dual Ethernet NIC that provides connectivity to the LAN side of the system. In a typical installation one Ethernet port is used for access to a management network; the other port is used for call access to the voice/modem/fax IP network. The edge server can be configured with two ethernet NICs for four port connectivity.

The IP telephony application that runs on the edge server sets up the call across the IP backbone, queries for IP addresses of remote (egress) Media Gateways and the SIP Proxy server, handles all call signalling, except for SS7, and initiates the creation of a Call Detail Record (CDR).

Other features include:

- H.323 and SIP support
- Auto registration (of the Media Gateway by the Gatekeeper or SIP Proxy)
- Support for in-band and out-of-band signalling
- Compliance with R2-MFC and Q.931/H.225/H.245 signalling standards
- A single edge server can be designated as both an ingress and an egress Gateway
- International Dialing Support -The CommWorks IP Telephony platform Release 2.3 supports international dialing using E.164 standards.
- Support for sending CDR's directly to the Accounting Servers when using SIP as call control mechanism.

System Capacity

One edge server card supports a different number of spans depending on the interface, the CODEC being used, and the frame size. As shown in the table below.

Table 5 Span Capacity per Media Gateway Chassis

CODEC	Frame Size	Frames per Packet	E1 Spans	T1 Spans	Voice Gateway Cards
G.711	20 (ms)	N/A	12	12	2
G.723.1 (6.3 kbps)	30 (ms)	N/A	8	8	1
G.729A	10 (ms)	1-3	12	12	2

Each Gatekeeper supports a different number of Media Gateways depending on the CODEC being used and the frame size. As shown in the table below.

Table 6 Number of Media Gateways Supported per Gatekeeper (or SIP Proxy)

Spans, Protocol	BHCA per Media Gateway	Media Gateways per Gatekeeper or SIP Proxy*
13 E1 spans, G.723.1	7800	16
12 E1 spans, G.711 (20 ms frame)	7200	17
6 E1 spans, G.711 (10 ms frame)	3600	34

The asterisks (*) indicates redundancy support.

If each Gatekeeper or SIP Proxy runs at 50% load, then it will fully support a full load from its redundant partner, if that partner goes down. Thus, while a SIP Proxy or Gatekeeper supports 250,000 BHCA, if only half of the BHCA is utilized, then you can implement a fully redundant system.

HiPer Network Management Card

The HiPer Network Management Card (HiPer NMC) provides a 10/100-Mbps Ethernet interface and manages the devices installed in the Total Control Hub under the direction of remote SNMP-based management software, such as IP Telephony Manager, CommWorks 5000, or HP OpenView.

Simple Network Management Protocol

The HiPer NMC uses the Simple Network Management Protocol (SNMP) to communicate with external management stations. The management station sends SNMP requests over IP, manipulating Management Information Bases (MIBs). The HiPer NMC carries out the requests and obtains results, and uses SNMP to return the results to the Management Station.

Network Management Card Functions

The Network Management Card (NMC) acts as an SNMP proxy for the other cards in the chassis which do not support SNMP. The NMC uses the Management Bus protocol to communicate to the installed chassis devices. The NMC provides this functionality within the chassis:

- NAC configuration management
- Automatic NAC configuration upon installation
- NAC configuration queries
- NAC software download upgrades
- Performance management
- Fault management

The NMC can also perform event management. Standard SNMP traps can be enabled to send an event notification or trap message to one or more management stations.

HiPer Network Management Card Functions

The HiPer NMC uses the Simple Network Management Protocol (SMNP) to communicate with the external management stations. The HiPer NMC acts as a SNMP Proxy for the other cards in the chassis which do not support SNMP. The Management Station sends SNMP requests over IP, manipulating Management Information Bases (MIBs). The HiPer NMC carries out the requests, obtains results and uses SNMP to return the results to the management station. Standard SNMP traps can be enabled to send an event notification or trap message to one or more management stations.

The HiPer NMC uses the Management Bus protocol to communicate to the installed chassis devices. The HiPer NMC provides this functionality within the chassis:

- NAC configuration management
- Automatic NAC configuration upon installation
- NAC configuration queries
- NAC software download upgrades
- Performance management
- Fault management
- Event management

HiPer DSP Card Set

The HiPer DSP card set consists of a T1 or E1 termination point (the T1/E1 NIC) and processing components (the HiPer DSP NAC). Each HiPer DSP terminates one T1 or E1 line. The HiPer DSP converts calls from pulse-code modulation (PCM) to digital voice packets and sends them to the edge server card set for further processing and distribution. At the far end of the call this process is reversed.

Features Include:

- G.711, G.723.1, and G.729A audio CODECs for PCM to voice/data/FAX conversion. (The default CODEC is G.711.)
- Jitter buffer to compensate for packet delay and/or lost packets.
- Q.931 ISDN D-channel signalling conversion to/from H.225 IP call control
- DTMF pass-through, H.245 compliant
- Caller ID support
- T1-PRI, E1-PRI, and E1-R2 support

- T.38 Real-time FAX over IP (G.723.1 and G.729A CODEC only.)—The edge server card can receive UDPL frames from the HiPer DSP, encapsulate them in a UDP datagram and send them to the destination edge server card. The edge server card can also receive a datagram from the LAN UDP that contain UDPTL frames and send them to the appropriate HiPer DSP.
- Auto-detection of Voice, FAX, Data—Depending upon which CODEC is configured for a call, the Gateway can automatically detect and set up voice, FAX, and data calls. For further detail, see Chapter 1 to the *Total Control 1000 Media Gateway Guide*.
- T1-PRI, E1-PRI, E1-R2, SS7 IMT Interworking - The Media Gateway supports connections between dissimilar Telco connections. This means that the ingress Gateway and the egress Gateway to which it communicates to complete a call do not need to have the same Telco interface for the call to be completed. For example; an ingress Gateway with T1-PRI lines connected to its HiPer DSPs can complete a VoIP call to an egress Gateway that has T1-PRI, E1-PRI or E1-R2 connections.

H.323 Gatekeeper

The Gatekeeper runs on a stand-alone Windows NT 4.0 Server or Windows 2000 Server and provides centralized call control, call routing, and overall system command and control.

The Gatekeeper application runs as a Windows service that:

- Registers and deregisters Media Gateways
- Assists Media Gateways in call setup and teardown
- Manages access to Media Gateways, identifies Back-end Servers, collects operational statistics, and generates traps
- Balances loads when there are multiple egress Media Gateways
- Consults the Directory Mapping Server to provide ingress Media Gateways with egress IP addresses that map to dialed telephone numbers
- Assembles Call Detail Records (CDRs) and logs them to Accounting Servers

When the Gatekeeper service starts, it logs an event in the Windows Event Viewer; this generates an SNMP trap. The Gatekeeper also generates traps when it finds each message queue and when it is ready to register Media Gateways.

When using the direct routed call model, the Gatekeeper is capable of supporting at least 250,000 Busy Hour Call Attempts (BHCA).

In IP Telephony Manager, the Media Gateway can be configured to use the Gatekeeper Routed Model. This means that if there is a Gatekeeper crash, active calls are dropped. However, if two Media Gateways are registered with different Gatekeepers, and one Gatekeeper is using Routed Call signalling, the egress Gateway supports the reception of an Admission Reject (ARJ) with a cause code of routeCallToGatekeeper. The Media Gateway also supports sending a facility message to have the call rerouted through the Gatekeeper. With the Routed Model, both Q.931 and H.245 signalling are routed. The default is Direct Routed.

SIP Proxy Server

In general, a proxy interprets, and if necessary, rewrites a request message before forwarding it. Within a Session Initiation Protocol (SIP) CommWorks IP Telephony System configuration, the SIP Proxy Server acts as both server and client for the purpose of making requests on behalf of other clients. Requests are serviced internally or passed on, possibly after translation, to other servers.

Specifically, the SIP proxy:

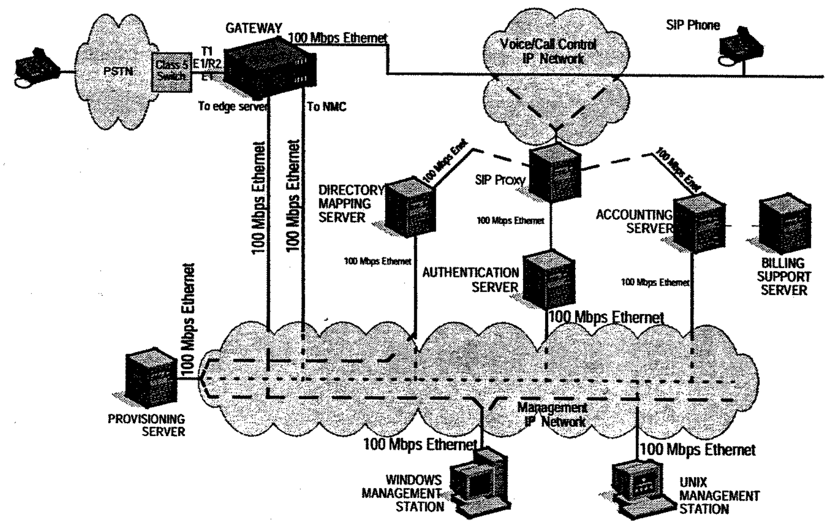
- Registers clients (SIP phones, SIP enabled Media Gateways, and other SIP devices).
- Manages call setup on- and off-net
- Looks to the subscriber database (Directory Mapping Server) for E.164 to IP address translation for both on-net and off-net calls

Major features of the CommWorks SIP Proxy Server include:

- RFC 2543 bis-02 compliance
- Sequential forking
- Call forwarding unavailable and call forwarding ring no answer support
- UDP and TCP request acceptance. Also registration on multicast.
- Proxy server, registration server, and redirect server support
- Transaction stateful and call stateful (proxy routed) call model support
- Legal loop detection, Via hiding, Expires timer, Max Forwards feature support
- Telnet support, via port 1822, to configure SIP proxy parameters.
- Support sending CDR's to the Accounting server directly when using SIP as the call control mechanism.

Figure 5 shows a typical CommWorks IP Telephony System configured for SIP.

Figure 5 VoIP SIP System Diagram



The SIP Proxy Server can be configured for either state-full or stateless operation:

- State-full—The SIP Proxy Server holds information in regard to the set-up and tear-down of the call.
- Stateless—The SIP Proxy Server processes a message and forgets everything else in regard to the call, until the arrival of next message.

Refer to *CommWorks 4220 SIP Proxy Server Guide* for more information.

Back-end Servers

This section describes the Back-end Servers.

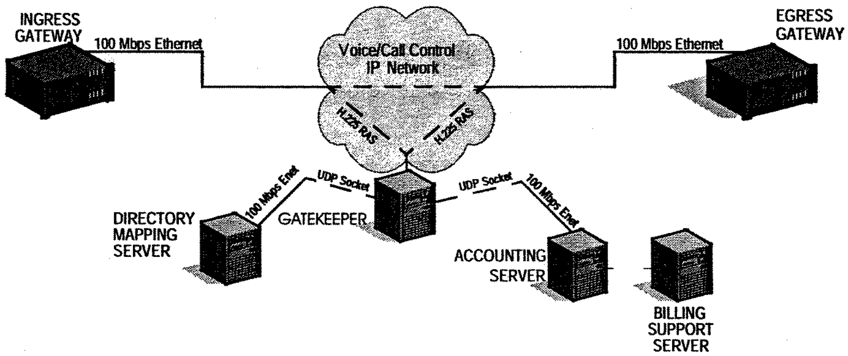
The Back-end Servers described are:

- Directory Mapping Server
- Provisioning Server
- Accounting Server
- Billing Support Server

Directory Mapping Server

The Directory Mapping Server runs on a Windows NT 4.0 Server or a Windows 2000 Server with Microsoft SQL Server 7.0. The Gatekeeper and the SIP Proxy calls upon the Directory Mapping Server mapping database when it needs to know the IP address of a destination Media Gateway. The Directory Mapping Server responds with a prioritized list of destination Gateways that are available to complete the call. The Gatekeeper selects one of the Media Gateways based on port availability.

Figure 6 Network Components



The Directory Mapping Server interfaces with the Gatekeeper using a proprietary User Datagram Protocol (UDP) sockets interface over IP. The Directory Mapping Server interfaces with the Provisioning Server using (SQL) over IP.

The Directory Mapping Server contains a database that maps destination telephone numbers (E.164 format) to a list of egress Gateways. When a Gatekeeper requests a list, the Directory Mapping Server responds with a prioritized list of egress Gateways that can complete the call. The Directory Mapping Server also does dialed number translation and format checking. It supports the North American Numbering Plan (NANP) and international numbering plans within selected countries.

Provisioning Server

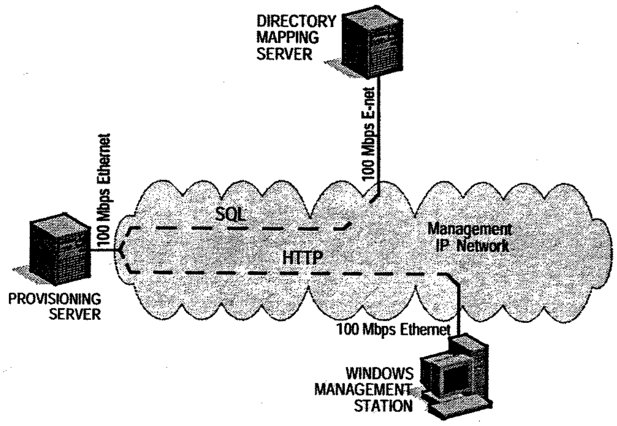
The Provisioning Server provides a means for network administrators to configure the Directory Mapping Server. Typical tasks that you can do from the Provisioning Server are assigning Media Gateways to Gatekeepers and assigning routes to Gatekeepers or SIP Proxy.

The Provisioning Server runs on a Windows NT 4.0 server or a Window 2000 Server and stands between the Directory Mapping Server, with which it communicates using SQL over IP, and a Windows PC running Microsoft Internet Explorer, with which it communicates using Dynamic HyperText Markup Language (DHTML) and JavaScript. For a Provisioning database, a Microsoft SQL Server must be on the network and available to the Web Provisioning Server.

Windows computers that run Internet Explorer contact the Provisioning Server by IP address. The Provisioning Server runs a web server application. Because the Provisioning Server uses ActiveX controls, Administrative clients must run Microsoft Internet Explorer on a Windows PC.

You can assign user names and passwords to protect the Provisioning Server from unauthorized use.

Figure 7 Provisioning Server in the VoIP Network



Accounting Server

The Accounting Server runs on a Windows NT Server or a Window 2000 Server with Microsoft SQL Server 7.0 or Windows 2000 server. The SIP Proxy or Gatekeeper sends Call Detail Records (CDRs), which are initiated by the Media Gateways, to the Accounting Server message queue. (In a SIP setup, the Gatekeeper is replaced with a proxy server. The Media Gateway, therefore, communicates directly with the Accounting Server.) The message queue stores CDRs until the database is ready to accept them. The message queue then passes the data to an SQL database.

Each successfully completed call results in four CDRs: ingress start, ingress end, egress start, and egress end. CDRs can be used for billing, service-level analysis, monitoring, and trouble locating and clearing.

Call Detail Records

During a normal call, four CDRs are logged into the table in the database on the Accounting Server. One CDR is logged at call initiation and one at call termination from each of the ingress and egress Gateways.

The Billing Support Server combines the four CDRs into a single super CDR for use by an external billing system.

Super Call Detail Records

The Super CDR merges all the CDRs that belong to a call. The four CDRs generated in a call are:

- Ingress call open
- Egress call open
- Ingress call close
- Egress call close

The Super CDR is stored in a new database that is created on the Billing Support Server. The CDR data is transferred into the new database by a Data Transformation Service (DTS) procedure.

Billing Support Server

The Billing Support Server is a specialized Accounting Server that is dedicated to extracting CDRs from the primary Accounting Server. The Billing Support Server then processes the CDRs into Super CDRs (the four CDRs that are generated for each call become one). Super CDRs are available to the proprietary accounting and billing systems of telephone companies, or to a third party accounting and billing system.

SNMP Management Subsystem

SNMP provides the primary means of configuring, upgrading, and gathering operational data from the components of the CommWorks IP Telephony platform.

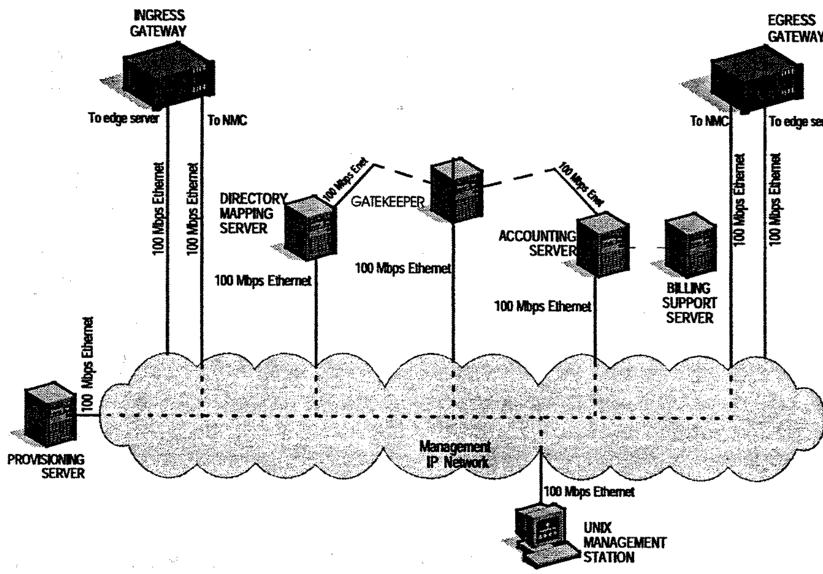
The IP Telephony Manager is the CommWorks SNMP element management application; it can manage the following CommWorks components:

- Gatekeeper
- Directory Mapping Server
- Billing Support Server
- Accounting Server
- Provisioning Server
- Media Gateways
- SIP Proxy
- HiPer DSP
- HiPer NMC

The Network Management Card acts as a proxy agent for the rest of the cards and systems within the Media Gateway, including the edge server cards.

You can use a third-party SNMP application to monitor the network status and to monitor alarm services. Either IP Telephony Manager integrated with HP OpenView on the HP-UX and Sun Solaris platform or CommWorks 5000 Network and Service Management system can be used to provide these features. You can also use the CommWorks 5000 Network and Service management system for this purpose.

Figure 8 SNMP Management Subsystem

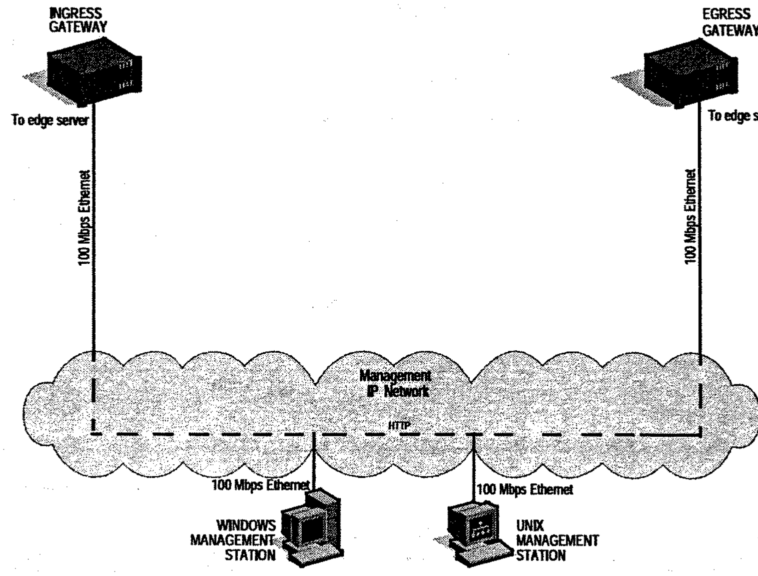


Real-time Media Gateway Operating Statistics

The edge server cards in the Media Gateways run a web server that provides operating statistics and Windows event log messages in real time. You can use the Web server without disrupting call processing.

You access the web server by using the IP address of the edge server card and any web browser that is on the same IP network as the edge server card.

Figure 9 Media Gateway Web Access



Management Workstations

Some management applications run on UNIX (HP-UX or Sun Solaris) workstations and some run on Windows.

Windows Management Workstation

You use the Windows management workstation to access all Windows NT components in the system. To manage the entire system from one workstation, you can install an X-Windows client, such as Hummingbird Exceed and then run applications from the UNIX management workstation.

You use Internet Explorer to access the Provisioning Server from which you can configure the Back-end Servers; you also use Internet Explorer to access the web interface on the ESPs from which you can view statistics and Windows NT event log messages.

UNIX Management Workstation

You can use HP OpenView or CommWorks 5000 (on Solaris) to monitor the status of all elements in the system and to act as an alarm server.

You use IP Telephony Manager to configure and monitor the components of the CommWorks system that do not use a Windows NT or Windows 2000 operating system, including configuring operational parameters, upgrading software and doing configuration backup and restore.

Table 7 Management Software

Software Package	Operating System	Function
Network management application, such as HP OpenView or CommWorks 5000	■ HP-UX ■ Sun Solaris	General network monitoring and alarm services
IP Telephony Manager	■ HP-UX ■ Sun Solaris	SNMP management and software upgrades of all CommWorks components of the CommWorks IP Telephony platform
Internet Explorer	Windows	Configuration of Directory Mapping Server, when used to access the Provisioning Server
Any web browser	Any	Gathering statistics from edge server, viewing Windows NT event log messages

Other Features

This section describes other features of the CommWorks IP Telephony Platform.

International Dialing Support

The CommWorks IP Telephony platform supports international dialing based on the E.164 standard. You configure and store country information in the edge server card. For more information, see the *Total Control 1000 Media Gateway Guide*.

T.38 Real-time Fax Over IP

The CommWorks IP Telephony platform supports real-time fax over IP. The Media Gateway card in the Total Control Hub (TCH) can receive UDPTL frames from the HDM, encapsulate them in a UDP datagram, and send them to the destination Media Gateway card. The Media Gateway can also receive datagrams from the LAN UDP that contain UDPTL frames and send them to the appropriate HDM.

Distributed Directory Mapping Server

The Gatekeeper supports a Distributed Directory Mapping Server feature. This means that when there are multiple Directory Mapping Servers in the network, if the Directory Mapping Server returns only the IP address of the egress Gatekeeper, the ingress Gatekeeper can still set up a call.

Real-time Billing

The CommWorks IP Telephony platform supports real-time billing. When a call is completed, the system can pass the CDR to a third party billing system through the billing support server for updates to the account.

Call Progress and Tone Generation

The system supports multiple and configurable call progress tones to the user including dial, busy, ring-back and congestion tones.

2 CALL FLOW

This chapter contains call flow information for standard call setup and normal call disconnect.

The types of call flows discussed are as follows:

- H.323/PRI Call Flow
- H.323/SS7 Call Flow
- SIP/PRI Call Flow
- SIP to SIP Call Flow
- SS7 and SIP Proxy Call Flow

H.323 Call-Control Signaling Path

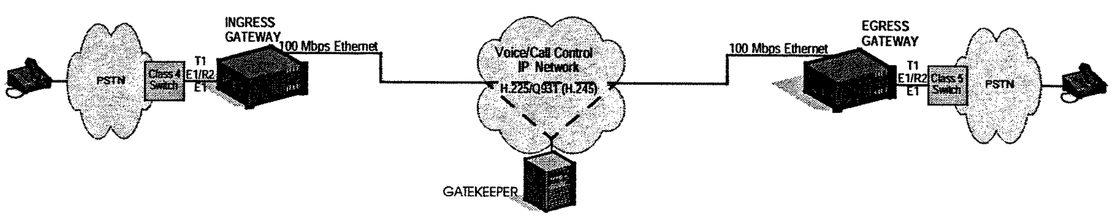
The Gateway converts Call Control messages from the T1 or E1 line to H.225; H.225 is a transport layer IP protocol for call control. First the HiPer Digital Signaling Processor (DSP) card converts messages into the internal packet bus protocol; then the Gateway converts the messages from the packet bus protocol to H.225.

The Gateways use the H.225 FastStart connection method; this reduces the effort of setting up an H.245 logical channel. If the Gateways reject FastStart, they use standard H.245 logical channel setup.

The Gateways and the Gatekeeper exchange H.225 Registration, Admission, and Status (RAS) messages.

Figure 10 shows the relationship between Q.931 Call Control Messaging and the H.225.0 v2 packet-based call signalling protocol.

Figure 10 Call-Control Signalling Path



H.323/PRI Call Flow

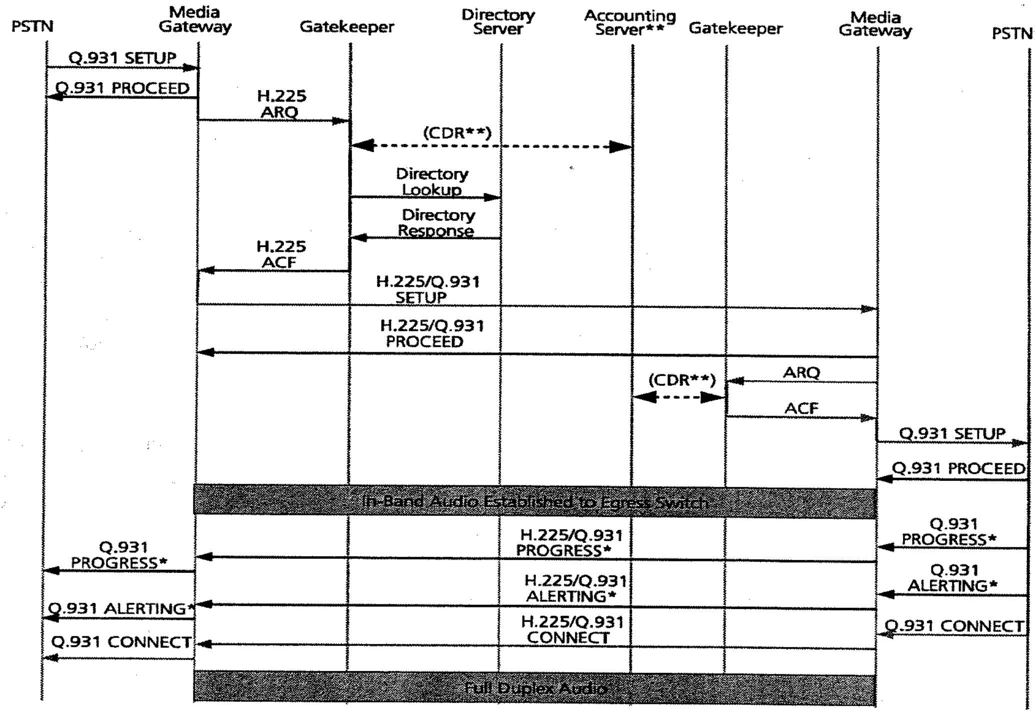
After setup between the PSTN and the ingress Media Gateway is complete, and after the ingress Media Gateway has registered with the Gatekeeper, the ingress Media Gateway sends an admission request containing the dialed number to the Gatekeeper. The Gatekeeper passes this request on to the Directory Mapping Server and logs a CDR to the Accounting Server, indicating that a call attempt is being made.

If the Directory Mapping Server sends back a lookup confirmation message containing egress Media Gateway addresses, the Gatekeeper passes the addresses on to the Media Gateway with an admission confirmation message. The ingress Media Gateway then sends a setup message to the egress Media Gateway, which responds to the ingress Media Gateway with a Proceed message.

When the egress Media Gateway sends the receiving Gatekeeper an admission request message, the receiving Gatekeeper responds with an admission confirmation if the receiving Gatekeeper and Media Gateway successfully register.

Finally, the receiving Media Gateway passes progress, alerting, and connect messages from the receiving PSTN to the ingress Media Gateway, the ingress Media Gateway passes these messages to the initiating PSTN, and full duplex audio is enabled.

Figure 11 VoIP Successful Call Setup With Direct Routed Call Model



* Optional message.
** Accounting Server is optional when the Gatekeeper is configured not to pass CDR from GW to Accounting Server.

Figure 11 assumes a Q.931 interface from each PSTN.

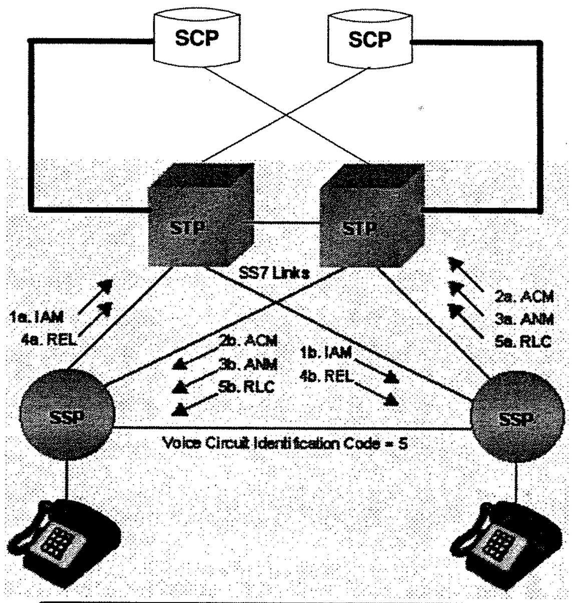
H.323/SS7 Call Flow

This topic discusses a basic H.323 and SS7 call control. Figure 12 illustrates the SS7 signaling associated with a basic call.

1 When a call is placed to an out-of-switch number, the originating Signal Switching Point (SSP) transmits an ISUP initial address message (IAM) to reserve an idle trunk circuit from the originating switch to the destination switch (1a). The IAM includes the originating point code, destination point code, circuit identification code (circuit "5" in Figure 12), dialed digits and, optionally, the calling party number and name. The SCP accepts queries for enhanced services from the SSP and returns the requested information to the originator of the query.

In the example below, the IAM is routed via the home STP of the originating switch to the destination switch (1b). Note that the same signaling link(s) are used for the duration of the call unless a link failure condition forces a switch to use an alternate signaling link.

Figure 12 Basic SS7 Signaling



Key:
SSP = Service Switching Points
STP = Signal Transfer Points
SCP = Service Control Points
——— = Voice Circuits
▬▬▬ = SS7 Signaling Links

2 The destination switch examines the dialed number, determines that it serves the called party, and that the line is available for ringing. The destination switch rings the called party line and transmits an ISUP address complete message (ACM) to the originating switch (2a) (via its home STP) to indicate that the remote end of the trunk circuit has been reserved. The STP routes the ACM to the originating switch (2b) which rings the calling party's line and connects it to the trunk to complete the voice circuit from the calling party to the called party.

In the example shown above, the originating and destination switches are directly connected with trunks. If the originating and destination switches are not directly connected with trunks, the originating switch transmits an IAM to reserve a trunk circuit to an intermediate switch. The intermediate switch sends an ACM to acknowledge the circuit reservation request and then transmits an IAM to reserve a trunk circuit to another switch. This processes continues until all trunks required to complete the voice circuit from the originating switch to the destination switch are reserved.

3 When the called party picks up the phone, the destination switch terminates the ringing tone and transmits an ISUP answer message (ANM) to the originating switch via its home STP (3a). The STP routes the ANM to the originating switch (3b) which verifies that the calling party's line is connected to the reserved trunk and, if so, initiates billing.

4 If the calling party hangs-up first, the originating switch sends an ISUP release message (REL) to release the trunk circuit between the switches (4a). The STP routes the REL to the destination switch (4b). If the called party hangs up first, or if the line is busy, the destination switch sends an REL to the originating switch indicating the release cause (e.g., normal release or busy).

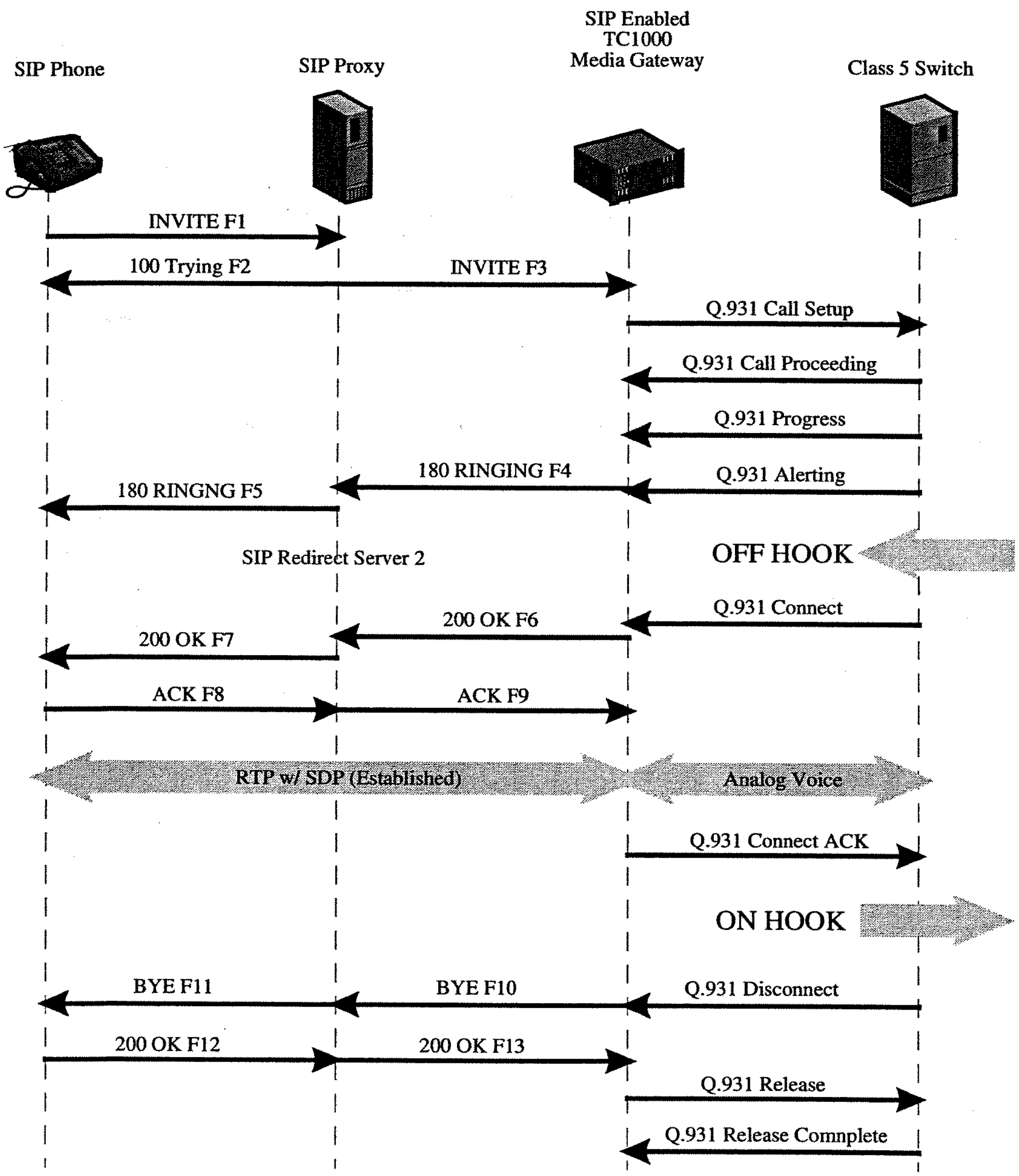
5 Upon receiving the REL, the destination switch disconnects the trunk from the called party's line, sets the trunk state to idle, and transmits an ISUP release complete message (RLC) to the originating switch (5a) to acknowledge the release of the remote end of the trunk circuit. When the originating switch receives (or generates) the RLC (5b), it terminates the billing cycle and sets the trunk state to idle in preparation for the next call.

ISUP messages may also be transmitted during the connection phase of the call (i.e., between the ISUP Answer (ANM) and Release (REL) messages.

SIP/PRI Call Flow

When a SIP device initiates a call to a destination that is not a SIP device, call flow progresses as shown in Figure 13.

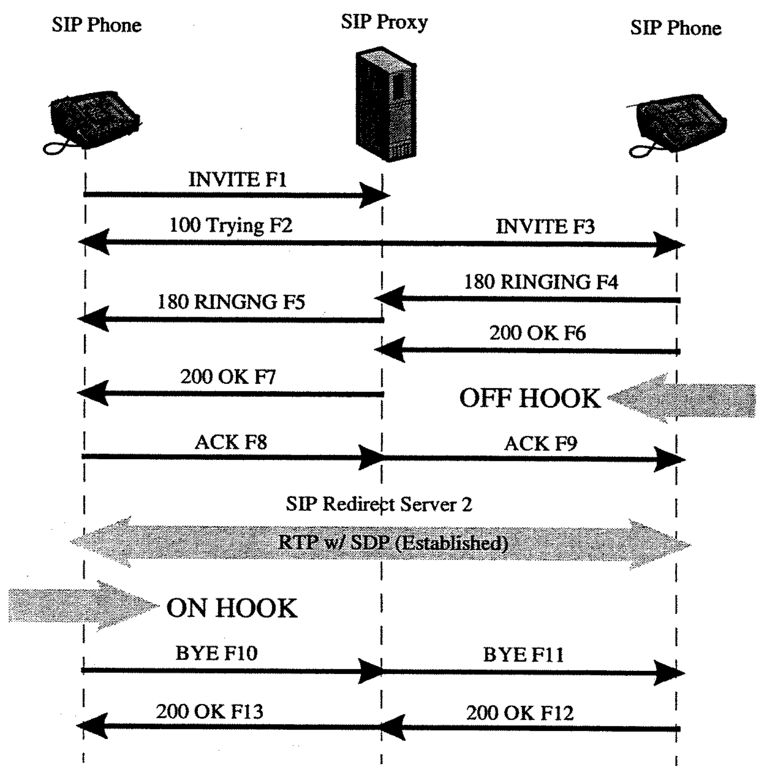
Figure 13 SIP-to-PSTN Call Flow



SIP to SIP Call Flow

When a SIP device initiates a call to another SIP device, call flow progresses as shown in Figure 14.

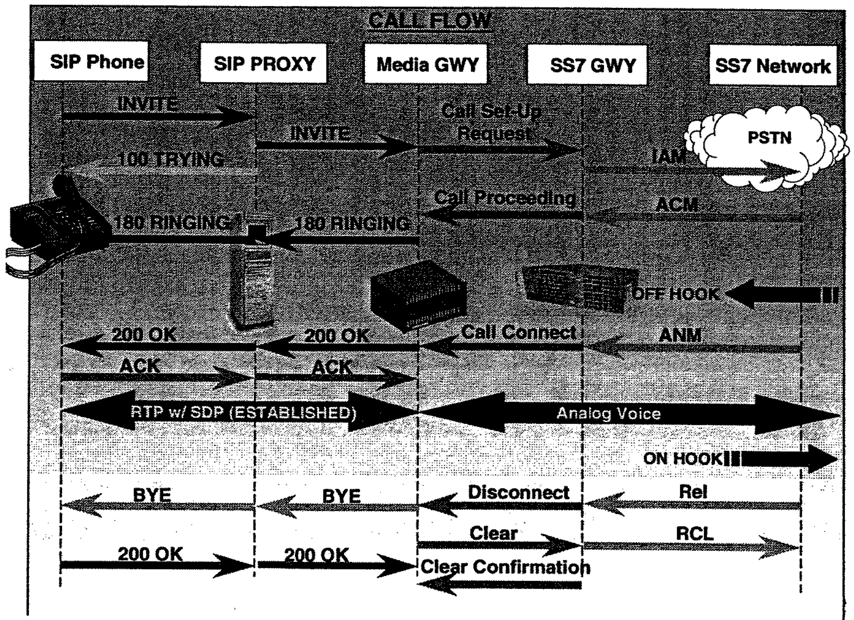
Figure 14 SIP-to-SIP Call Flow



SS7 and SIP Proxy Call Flow

Figure 15 illustrates the call flow when SIP, SS7, and a Media Gateway are placed on the system.

Figure 15 Call Flow Using SS7 and SIP Proxy



3

Networking Requirements

This chapter provides IP addressing, span, and ethernet requirements for the CommWorks IP telephony platform.

This chapter contains the following topics:

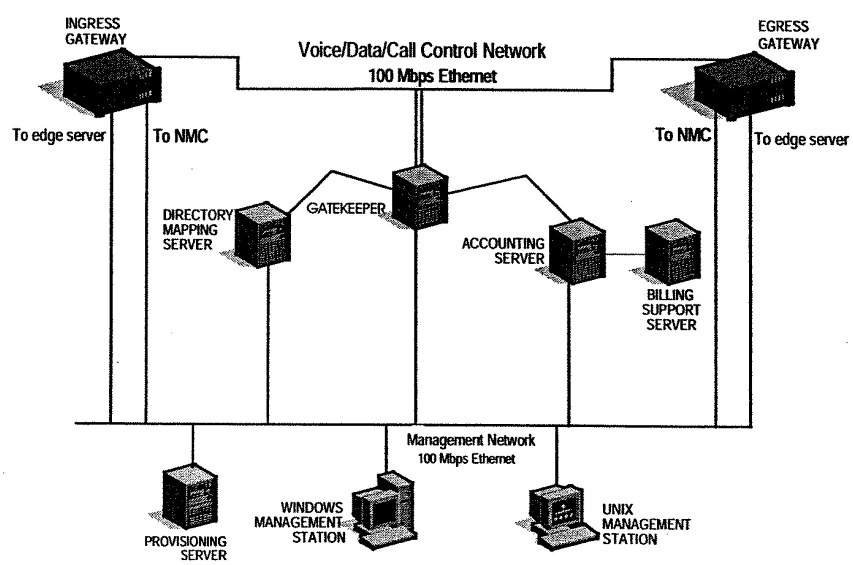
- Network Planning and IP Addressing
- Span Requirements
- Ethernet Requirements

Network Planning and IP Addressing

At a minimum, voice (plus modem, fax, and call-control) traffic should be separated from management (SNMP, TFTP) traffic.

For a small environment, such as a test lab, only two ethernet segments are required. Connect all management interfaces to one ethernet segment and all voice network interfaces to a different ethernet segment.

Figure 16 Network Planning Example



Some system components are designed to be *dual-homed*, that is, to have two interfaces: one to the voice network and one to the management network. Directing the traffic to one port or the other using static routes. A static route is only defined on the Media Gateway and forces the RTP data to be routed to the specified Media Gateway. See the *Total Control 1000 Media Gateway Guide* for more details.

Table 8 Dual Homing Chart

System Component	Voice Network	Management Network
EdgeServer Pro	Yes	Yes
Network Management Card	N/A	Yes
Gatekeeper	Yes	Yes
SIP Proxy	Yes	Yes
Directory server	Yes	Yes
Accounting server	Yes	Yes
Billing Support Server	Yes	Yes
Provisioning server	Yes	Yes
Windows Management Station	Yes	Yes
UNIX Management Station	N/A	Yes

For static routes to work, the two networks (voice and management) must be different IP networks or IP subnets.

Span Requirements

This section lists information useful for cabling and installing Telco spans to the Media Gateway.

Span Line Interfaces

The span interface on the HiPer DSP T1/E1 NIC has the following pinouts:

Figure 17 HiPer DSP T1/E1 NIC, RJ48C Span Connector Pinouts